

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

November 10, 2019

Richard B. Russell Federal Building
2211 United States Courthouse
75 Ted Turner Drive, SW
Atlanta, GA 30303-3309

FILED IN CLERK'S OFFICE
U.S.D.C. - Atlanta

NOV 20 2019

JAMES N. HATTEN, Clerk
By:  Deputy Clerk

Dear Honorable Chief Judge Thomas Thrash Jr.,

I am writing to object to the proposed settle between the FTC and Equifax. I believe some of the terms are too ambiguous and need more details so victims can make well informed decisions. I think some of the terms are too shallow and don't provide enough consideration for victims. Finally, I feel some problems received no treatment but need to be addressed.

Equifax had the opportunity to protect the data for a fraction of the cost but the company squandered it. After reading the settlement and some of the artificially small caps on payments for services and costs I developed the impression the company is trying to push most of the risk and loss onto victims and tax payers. I sincerely hope the government is wise to what is going on here.

If the Court is not aware of the problems and challenges victims of a data breach face, then I respectfully recommend *Identity Theft in Maryland: Shifting Circumstances – Continuing Challenges*.¹ It is written by the former Attorney

¹ http://dls.state.md.us/data/polanasubare/polanasubare_coucrijuscivmat/Identity-Theft-2013.pdf

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

General of Maryland and is one of the more comprehensive treatments I have read. From the document:

Criminals are using PII, however, not just to steal money but to steal health care, prescription drugs, citizenship status, tax refunds, unemployment benefits, and even driving privileges. A relatively recent disturbing trend is the commission of identity fraud to avoid sex offender registration requirements.

Background

The Equifax data breach occurred mid-May to July 2017, and was announced September 2017². Visa and Mastercard reported the suspicious activity as early as late 2016.³ The breach affected approximately 147 million individuals. The breach was attributed to an unpatched server. In particular, Apache Struts Vulnerability CVE-2017-5638. The vulnerability was disclosed in March 2017.

Many people in my field of Information Security were surprised Equifax was not patching their servers in a timely manner. Patching servers with security updates like for CVE-2017-5638 is "System Administration 101." All levels of system administrators are taught number one threat to an organization's data is unpatched servers. Even junior administrators know to patch their servers

After the breach but before it was disclosed some officers of the company "doubled down" on illegal activity and sold some their shares in the company to

² <https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/>

³ <https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

avoid the upcoming losses. At least one was charged with insider trading and is serving prison time for it.⁴

According to FTC statistics, identity theft complaints declined in 2016⁵, but rose 14% in 2017⁶ and rose an additional 24% in 2018⁷. Statistics indicate information from the Equifax data breach is actively being used by bad actors.

While there were a number of breaches in 2017, the majority of them did not include names and social security numbers. And those that included names and social security numbers did not achieve the magnitude of the Equifax breach. The second through fourth place finishers are America's JobLink, 4.8 million records; TIO Networks, 1.6 million; and Washington State University, 1 million records. Equifax contributed over 92% to the records lost social security records in 2017. Combined, the runner's up account for less than 5% of the records lost social security records in 2017.

Ambiguous Terms

The terms of the settle agreement are ambiguous. There are several instances of ambiguity that should be fixed before proceeding with the settlement.

First, the length of credit monitoring is variable. It could be as little as 4 years or could be as long as 10 years. If more people opt for the credit monitoring than anticipated, then more money needs to be added to the fund. The length must be

⁴ <https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading>

⁵ <https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints>

⁶ <https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers>

⁷ <https://www.ftc.gov/news-events/press-releases/2019/02/imposter-scams-top-complaints-made-ftc-2018>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

fixed and clearly stated. Otherwise consumers do not know what they may receive.

Second, the monetary compensation option is variable. It could be as much as \$125 USD or as little as a few dollars. If more people opt for the monetary compensation than anticipated, then more money needs to be added to the fund. The dollar amount must be fixed and clearly stated. Otherwise consumers do not know what they may receive.

Third, the settlement does not specify the details of monitoring. It is not clear what Equifax, Experian, and TransUnion will monitor, and what will be provided to a victim in the report. It is also not clear how some things are going to be monitored.

An example of “how something is going to be monitored” is a bank account. Bank accounts are fundamental and most people have them. However, banks don’t submit customer information or checking and savings account information to reporting agencies. The reason is simple – the banks don’t want their customers poached by a competitor. There is no mechanism in the current settlement to detect unauthorized bank accounts.

Now suppose bad checks are written on the fraudulent bank account. Credit reports don’t include bounced check information. There is no mechanism in the current settlement to detect bounced checks from fraudulent bank accounts.

So it is not clear to me how a victim will find out about additional bank accounts and bad checks given the monitors don’t receive the information. There is a way to do detect the fraud in many cases, but the option is not available in the

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

settlement. In fact, Wells Fargo exploited this fact and opened fake bank accounts using their banking customer's identities.⁸

In an effort to remove confusion and ambiguity, Walton wrote to the FTC in October and asked for details of what was being monitored and exemplary reports from the agencies. Walton also asked the items be submitted with the settlement for the Courts approval. Walton was directed to the Equifax Data Breach FAQ⁹ which lacked the information. The Administrator's site also lacked the information. The information also was not provided to the Court for approval.

To put the problem of ambiguous terms in perspective: would the Judge, the FTC lawyers or the Equifax lawyers agree to a mortgage or credit card if the term was "some interest rate" and subject to change at any time? I'm guessing no. I'm speculating attorney would want an exact interest rate with exact terms stated up-front and in writing.

Credit Monitoring

The settlement claims to offer "Up to 10 years of free credit monitoring", and also states "at least four years of free monitoring of your credit report at all three credit bureaus."¹⁰ There are several problems with these terms.

First, the bad actors who are using the stolen identities do not observe "4 year rule" or the "10 year rule". The bad actors will commoditize the stolen identity as long as it is bearing fruit. A victim who is being actively exploited needs a lifetime of protection.

⁸ <https://www.forbes.com/sites/maggiemcgrath/2016/09/08/wells-fargo-fined-185-million-for-opening-accounts-without-customers-knowledge/>

⁹ <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>

¹⁰ <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement#FAQ5>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Second, the term assumes bad actors will use the stolen identity immediately. Economic theory tells us if too many stolen identities are dumped on the market at once, then the value (price) for a stolen identity will drop. I believe the thieves will keep the value (price) for a stolen identity high, so they will limit the rate that stolen identities are released and used. The FTC statistics seem to indicate this pattern since identity theft complaints are growing more than expected over time. A potential victim who could be exploited needs a lifetime of protection.

Interestingly, baseball player agents recognized the same economic pressures as the data thieves, and that is why collective bargaining in baseball does not allow a player to enter free-agency until 3 years. Agents realized too many super-star free agents hitting the market too frequently will drive down the cost of the player.

Third, some victims are infants and children. They will not learn of the damage caused by the data breach until long after the 4 years or 10 years have expired. A victim who is being actively exploited or potential victim who could be exploited needs a lifetime of protection. A child victim who could be exploited needs a lifetime of protection.

Fourth, the Fair Credit Reporting Act (FCRA) cited in the settlement allows derogatory entries on a credit report for 7 or 10 years. The settlement only ensures up to four years of monitoring. There is a six year gap that needs to be closed based on Congress' rendering of interstate commerce laws in this area.

Breach Disclosure

The Equifax data breach is unique in that a credit reporting agency suffered the breach. Equifax controls their database and can place entries in their database at

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

will¹¹. The settlement does not require Equifax to report the stolen identity event on the consumer's credit report. There are several problems with the missing information.

First, the lack of an "Equifax 2017 data breach" entry means an individual's credit report is incomplete and does not paint an accurate picture of the individual. Known information is being intentionally omitted. Companies and agencies that receive the reports cannot use the information to assess an individual for credit worthiness, assess an individual for employment, or assess an individual for insurance because the information is missing.

Put another way, a fully qualified individual may be disqualified because of an unexplained derogatory entry due to an identity theft incident. The receiver of the credit report is no wiser and interprets the entry against the victim because necessary information is missing from the report.

As a concrete example, suppose the stolen information is used to open a checking account and attend a doctor's visit. Further, suppose the identity thief writes a bad check at the doctor's office. A credit report won't report the bank account and won't report the bad check. However, a collection agency could report the unpaid medical bill and subsequent debt collection. The events will negatively affect the individual even if the events took place 2500 miles away from the victim.

And god save the individual if he or she is a candidate for a law enforcement position, a sensitive military MoS, or a top secret clearance; and the doctor's visit

¹¹ In contrast the Anthem data breach, which was another massive breach, did not have this unique facet. Anthem did not control credit reporting databases, and could not compel credit reporting agencies to report the incident on a consumer report.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

was for a venereal disease or drug overdose or something similarly distasteful. A thorough background check will uncover these fallacious facts, and it won't be obvious to the investigator that these facts are actually false and part of an identity theft. A victim trying to explain this to an investigator is too late. It needed to be fixed before the investigation.

Second, the missing "Equifax 2017 data breach" entry means an individual must be aware of a derogatory entry from the breach before it can be fixed or explained. This places an individual at a disadvantage in the market by default. Here, the market could be any market like home loan, credit card rate or job market. Being disadvantaged "out of the box" is simply unfair to the individual.

Third, every individual affected by the report must write to Equifax every three months and request that their credit report include the information. A victim should not have to do anything special; the protection and entry should simply be present. It is not clear to me if a credit reporting agency like Equifax will honor such a request like "Please include the statement, I was part of the Equifax Data breach in 2017 and my identity may be used fraudulently" if it is not mandated by the settlement. It is a burden the victims should not have to endure.

Fourth, the cash portion of the settlement has been reduced to proverbial pennies. Individuals who have to manually tend to this task will never be compensated for their time. In fact, the cash portion of the settlement is so small it may not even cover the cost of the postage stamps over time.

Finally, if Equifax claims to provide accurate information about an individual but fails to supply "Equifax 2017 data breach" entry in the report, then the information about an individual is incomplete and not accurate.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Missing Agencies

The settlement names three agencies for credit monitoring: Equifax, Experian, and TransUnion. The three credit reporting agencies have a limited looking glass and depend on other firms and institutions to feed the agencies data. If an agency lacks an appropriate data source then some information is unreported.

There are other agencies that perform better in certain areas of monitoring. For example Early Warning is credit reporting agency that is not on the list. Early Warning is a collection of the largest US banks that pool their customer databases and provide real-time risk management for financial transactions. If a bank account or credit card exists for a stolen identity – or an application is made for a bank account or credit card – then there is a good chance Early Warning will know about it and the three credit reporting agencies **will not** because Early Warning does not share the bank data.

It would benefit victims of the breach to obtain their Early Warning credit reports on a regular basis because Early Warning provides information not available to the three credit reporting agencies.

Summary Reporting

Credit reporting agencies like Equifax, Experian, TransUnion and Early Warning prepare different reports for different applications and different customers. Painting with a broad brush there are at least two types of reports: summary reports and detailed reports.¹²

¹² “Summary report” and “detailed report” is the exact language used by Early Warning.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Victims in this settlement will receive a quasi-summary report.¹³¹⁴¹⁵ Lenders, employers, law enforcement agencies, the military and insurers will often receive detailed reports. The disparity has several problems for victims.

First, the victims are provided different reports than others that request the reports, like law enforcement and background investigators. A summary report provided to the victims will lack information present on the detailed report seen by lenders, employers, law enforcement, military, insurers, etc.

Second, since victims have an abridged view of their information, and they may not have the opportunity to correct the incomplete, inaccurate or incorrect information. They may not even know there is a problem. A victim cannot correct what they don't know about.

Third, most people do not know there are different reports, and so they don't know to ask for the detailed or comprehensive report. In the case of Equifax, Experian, TransUnion, their example reports are summary reports with some details; and not detailed reports provided to lenders, employers, law enforcement, military, insurers, etc.¹⁶¹⁷¹⁸

In fact it is a practice at Early Warning to provide a summary report when someone asks for his or her credit report. The only time a person receives a detailed report is when they specifically ask for it.

¹³ https://www.equifax.com/pdfs/corp/Equifax_Optima_Sample_Report.pdf

¹⁴ https://www.experian.com/credit_report_basics/pdf/samplecreditreport.pdf

¹⁵ https://www.transunion.com/docs/rev/personal/Credit_Report_Explanations.pdf

¹⁶ https://www.equifax.com/pdfs/corp/Equifax_Optima_Sample_Report.pdf

¹⁷ https://www.experian.com/credit_report_basics/pdf/samplecreditreport.pdf

¹⁸ https://www.transunion.com/docs/rev/personal/Credit_Report_Explanations.pdf

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Early Warning is not alone. Equifax, Experian, and TransUnion's stock request form does not request the detailed or comprehensive report. It does not matter whether a consumer orders over the phone or sends the form by mail. The process does not offer the detailed report, so there is no way for a consumer to request the detailed report.

Disparity among Members

The settlement action covers roughly 147 million people in the United States. Unfortunately all class members are not treated equal. Credit Bureaus maintain "VIP Databases" of influential members of society. Influential members of society include politicians, judges, athletes, actors, actresses and musicians.

The reporting agencies **voluntarily** provide special treatment for the influential members of our society. Derogatory items are manually checked and confirmed, some derogatory items are not reported on an individual's credit report, and other derogatory information is removed from a credit report. In contrast most class members are not in the VIP database, they do not enjoy preferential treatment, and they are subject to unconfirmed reporting complete with the inaccuracies that follow. There are several problems here.

First, the credit bureaus give special treatment to VIP members for a reason. They want to ensure the status quo. Reporting agencies don't want to risk the ire of politicians who could write legislation against them. And they don't want athletes, actors and actresses taking up causes on social media which could lead to unwanted change in their business.

The bigger problem is, the agencies are perverting the political process and denying most members of society and all members of the class their due process.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

Some might even say the agencies are corrupting and influencing influential members of society.

The practice of influencing certain members of our society must stop so that all members of society and the class can enjoy the benefits of unbiased legislation and meaningful protections.¹⁹ The settlement agreement must stop the practice of influencing like this.

Second, all members of the class should receive the same treatment. I don't want to ask the court to dismantle the VIP database or the processes involved in maintaining the database. It is good the processes are in place, and it is good at least some individuals receive good care in these matters. Instead, I would like the settlement to ensure every individual receives the same handling as politicians, judges, athletes, actors, actresses and musicians. And as with influential members of society, all class members should enjoy the protections for life at no charge.

I first learned of the VIP databases years ago. I believe I was watching a financial crisis documentary. Bill Black was interviewed and spilled the beans on the VIP databases. I encourage the Court to discuss this further with Dr. William Black, J.D.²⁰ He can be found teaching at the University of Missouri.

Privacy

Members of the class must provide identifying information to enroll in the services stated in the settlement. The identifying information includes name,

¹⁹ The Electronic Frontier Foundation has several good position papers on this problem. The EFF does not directly attack the VIP databases. Rather, they discuss the gaps caused by inadequate legislation.

²⁰ Dr. Black is a J.D. and a professor of law at the University of Missouri. He is a former bank regulator and helped prosecute the folks responsible for the financial crisis in the mid-1980's, like Charles Keating. The US government declined his assistance after the 2008 meltdown. Not surprising, no criminal prosecutions were attempted in the US for the folks who were responsible for the melt down.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

social security number, address, phone number and email address. The reporting agencies may not have up-to-date information on an individual so this is a proverbial “gold mine” of information.

The problem is, some individuals may wish to remain private. Individuals in this group would include people who value their privacy, individuals who shun the practices of modern data collection, and individuals who are used to strong privacy protections, like those provided in European nations. It is tenuous to blame someone for not wanting to share their information in this instance. Information sharing is what got them here in the first place. Once bitten, twice shy, as the saying goes.

The settlement does not appear to place any restrictions on how the information is used after the victim identifies himself or herself. The settlement must ensure the personal information gathered for the purposes of the settlement remain private; and the information is not shared, sold or disseminated in any way.

Barriers to Service

I can relay this problem with firsthand experience. My apologies for the verbosity in this section. Credit reporting agencies place too many barriers and deny credit report requests by individuals.

In 2005 I was in a hit-and-run motorcycle accident. I was the motorcyclist. I had medical insurance and short term disability, but I did not have long term disability. I was out of work about two years while my back healed. My last surgery occurred in 2006 or early 2007, but were paid for by insurance.

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

During the two year time a credit card and loan were charged off. I had rainy day money but I used it to live on rather than pay bills. I accepted the events as "shit happens, and sometimes it happens to you."

In 2014 I failed to obtain a particular job I was very interested in. I performed a root cause analysis and concluded I needed more information to explain the events. My charge off occurred about a decade earlier so the charge-off should not have factored into the failed attempt due to limitations specified by FCRA.

I attempted to obtain my credit report from Equifax in June 2014. I first tried by phone and was denied by the automated phone system. I then tried in writing using the form from the Equifax website but the request was not fulfilled. Equifax did not bother sending me a denial letter. They simply did not respond.

Equifax does not have an office in my state so I could not visit a local office, show my driver's license or passport, and obtain the consumer report. Equifax does not provide a number to talk to a real person so I could not get more information from the company.

I suppose my next step was hire a lawyer and initiate an action in Federal Court. This is not a reasonable course of action for a reasonable person. Reasonable people accommodate reasonable requests, and reasonable people don't expect to spend \$10,000 USD to retain a lawyer to obtain a credit report guaranteed by Federal law.

There were too many barriers in the process.

Removing the barriers means a person can get to a local office, show identification, and obtain a detailed credit report from the office. For accessibility

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

purposes, it does not matter if the credit agencies open several local in each state. Or a victim can use a designated agent of a reporting agency to fulfill the request. The point is, there is a local place to go to obtain the report and talk to a real person if needed.

If the Court believes a victim will be able to easily obtain a credit report then it is probably mistaken. The settlement must ensure barriers are removed so victims can obtain a report in a timely manner.

SIRF Fraud

A byproduct of the data breach is identity theft and Stolen Identity Refund Fraud (SIRF)²¹. City, state and federal governments and tax payers are absorbing the costs associated of this data breach.

As the 9th Circuit Court of Appeals correctly recognized there is a “credible threat of real and immediate harm” after a data breach. The FTC statistics confirm the 9th Circuit Court of Appeals’ intuition. As reported by the FTC, something reversed the decline in identity theft complaints for 2016 and caused the 14% rise in 2017 and 24% rise in 2018. It was most likely the Equifax data breach since Equifax was responsible for over 92% of the social security numbers lost in 2017; and there are no other credible sources or explanations.

According to US Treasury, the United States losses over \$6 Billion USD a year in SIRF fraud²². The increased losses due to SIRF fraud for 2017 and 2018 were passed on tax payers. There are approximately 329 million people in the United States. 147 million or 44.6% are members of this class settlement.

²¹ <https://www.justice.gov/tax/stolen-identity-refund-fraud>

²² Treasury reports losses of over \$30 billion per year, but claims to recover over 80% of the losses

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

It appears the FTC did not study the problem or provide an explicit solution. Not collecting data and pretending a problem does not exist is disingenuous and unethical at best. I have stronger opinions on the matter, but I am going to keep them to myself. The Court needs complete and accurate information to evaluate the settlement, but it is completely missing here.

Correlating lost identity information from Equifax with SIRF fraud from Treasury is as simple as a database query. For each victim of the breach, report the dollar amount of the SIRF fraud in 2016 (pre-breach), 2017 and 2018 (post-breach).²³ Remove from the list anyone who was fraudulently active in 2016, or part of another breach like America's JobLink.

I believe the Court's ruling on the City of Chicago intersects here. If I am not misunderstanding the court's ruling, governments like the City of Chicago are part of this settlement and they have to make their claims as part of this settlement. Therefore, issues like SIRF fraud, loss of revenue and unfunded services needs to be addressed now for city, state and federal governments.

Data breaches in the private sector assign blame and hold the appropriate parties responsible. For example, Home Depot settled with banks for bank's losses due to the Home Depot data breach.²⁴ Tax payers, members of the class and government expect the same of Equifax. Equifax must take financial responsibility for the SIRF fraud and financial hardships it has caused.

²³ If my estimates are correct, tax payers and class members will pay out more for SIRF fraud then they will get back from the this settlement. It is a net loss for tax payers and class members.

²⁴ <https://fortune.com/2017/03/09/home-depot-data-breach-banks/>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

I generally don't make demands but I will in this case. I demand the FTC study the problem and release the "uncooked" statistics as part of the settlement. The statistics must anonymized information and include exact dollar amounts.

Profiteering

Equifax is one of the companies that provides risk management services to various treasuries and comptrollers offices, at both the state and federal levels. In the case of the Equifax data breach, the company introduced the disease and are now selling the cure.

My research indicates the names, addresses and social security numbers of victims were **not** provided to treasury and comptroller offices. State and federal agencies lacked critical information and were not able to place alerts on victim accounts nor monitor the accounts with heightened vigilance. Instead Equifax is selling the information as a service to the state and federal governments.

This is not the only instance of Equifax profiteering. The company charged consumers for credit freezes through November 2017.²⁵ I am appalled the company was allowed to charge consumers for protections needed due to the company's own mistakes.

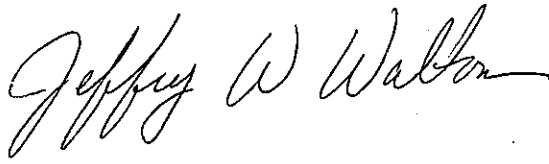
A settlement must eliminate the profiteering.

Closing

Thank you for reading this objection letter. I hope my concerns can be addressed.

²⁵ <https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html>

FEDERAL TRADE COMMISSION v. EQUIFAX INC.
Case 1:19-cv-03297-TWT

A handwritten signature in black ink, reading "Jeffrey W. Walton". The signature is written in a cursive, flowing style.

Jeffrey Walton

8482 Fort Smallwood Road

Unit B-103

Pasadena, MD 21122



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Equifax Data Breach Settlement

Share This Page

September 2019

Affected by the Equifax breach? File a claim now.

In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up to \$425 million to help people affected by the data breach.



If your information was exposed in the data breach, you can file a claim at EquifaxBreachSettlement.com for the benefits described below.

Not sure if your information was exposed? Use this [look-up tool](#) to see.

You can [file a claim](#) for:

Free Credit Monitoring and Identity Theft Protection Services

- Up to 10 years of free credit monitoring, including:
 - At least four years of free monitoring of your credit report at all three credit bureaus (Equifax, Experian, and TransUnion) and \$1,000,000 of identity theft insurance.
 - Up to six more years of free monitoring of your Equifax credit report.
(Previously, a cash payment was identified as an alternative to the free credit monitoring, but there are limited funds available. See [FAQ 4](#) for details.)
- If you were a minor in May 2017, you are eligible for a total of 18 years of free credit monitoring.

Cash Payments (capped at up to \$20,000 per person)

- For expenses you paid as a result of the breach, like:
 - Losses from unauthorized charges to your accounts
 - The cost of freezing or unfreezing your credit report
 - The cost of credit monitoring
 - Fees you paid to professionals like an accountant or attorney
 - Other expenses like notary fees, document shipping fees and postage, mileage, and phone charges
- For the time you spent dealing with the breach. You can be compensated up to \$25 per hour up to 20 hours. There are limited funds available so your claim may be reduced. See [FAQ 7](#) for more details.
 - If you submit a claim for 10 hours or less, you must describe the actions you took and the time you spent doing those things.
 - If you claim more than 10 hours, you must describe the actions you took AND provide documents that show identity theft, fraud, or other misuse of your information.
- For the cost of Equifax credit monitoring and related services you had between September 7, 2016, and September 7, 2017, capped at 25 percent of the total amount you paid.

Even if you do not file a claim, you can get:

Free Help Recovering from Identity Theft

- For at least seven years, you can get free identity restoration services. If you discover misuse of your personal information, call the settlement administrator at 1-833-759-2982. You will be given instructions for how to access free identity restoration services.

Free Credit Reports for All U.S. Consumers

- Starting in 2020, all U.S. consumers can get 6 free credit reports per year for 7 years from the Equifax website. That's in addition to the one free Equifax report (plus your Experian and TransUnion reports) you can get at AnnualCreditReport.com. [Sign up for email updates](#) to get a reminder in early 2020.

FAQs

1. **What is the deadline to file a claim?**
2. **When will I get my benefits?**
3. **How will I get my benefits?**
4. **I thought I could choose \$125 instead of free credit monitoring. What happened?**
5. **I don't want Equifax to have my data. What can I do?**

6. I don't want credit monitoring from Equifax. What are my options?
 7. How much of the settlement fund can be used to pay claims for time spent dealing with the data breach?
 8. I'm not sure I was affected by the data breach. How can I find out?
 9. What else can I do?
-

1. What is the deadline to file a claim?

You must file a claim by January 22, 2020.

2. When will I get my benefits?

The settlement administrator will not send out any benefits until they are allowed to do so by the court, which will be **January 23, 2020, at the earliest**. We will update this page, and send email updates, when we have more information.

3. How will I get my benefits?

For free credit monitoring, after final approval from the court, you will get an activation code with instructions. You can choose to receive this code by email or postal mail when you file your claim.

For cash payments, you can choose to get a check or debit card when you file your claim. It will be sent to your mailing address after final approval from the court.

4. I thought I could choose \$125 instead of free credit monitoring. What happened?

The public response to the settlement has been overwhelming. Because the total amount available for the alternative compensations is \$31 million, each person who takes the money option is likely to get a very small amount. Nowhere near the \$125 they could have gotten if there hadn't been such an enormous number of claims filed.

The free credit monitoring provides a much better value, and everyone whose information was exposed can take advantage of it. If your information was exposed in the data breach, and you file a valid claim before the deadline, you are **guaranteed** at least four years of free monitoring at **all three credit bureaus** (Equifax, Experian, and TransUnion) and \$1,000,000 of identity theft insurance, among other benefits. The market value of this product is hundreds of dollars per year.

You can still choose the cash option on the claim form, but you will be disappointed with the amount you receive and you won't get the free credit monitoring.

5. I don't want Equifax to have my data. What can I do?

Related News

- [FTC Encourages Consumers to Opt for Free Credit Monitoring, as part of Equifax Settlement](#)
- [Equifax to Pay \\$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach](#)



[ftc.gov](https://www.ftc.gov)

NOVEMBER 12, 2019

eff.org



Equifax Data Breach Update: Backsliding

After Equifax's calamitous 2017 data breach, its settlement with the Federal Trade Commission (FTC) and the private attorneys representing victims appears to offer two potential remedies to all 147 million American consumers affected: free credit monitoring, or if individuals already had free credit monitoring, an up to \$125 cash payment. The FTC directed consumers affected by the breach to a third-party website where they could quickly and easily file their claim.

At the time, EFF tepidly commented on the settlements' efforts to compensate consumers. But we also noted that the \$125 payments would come from a \$31 million fund, meaning that if all 147 million victims chose the payment, each person's payment would be reduced on a *pro rata* basis to as little as 21 cents each.

Indeed. Less than one week after it announced the settlement, the commission began encouraging consumers to forego the monetary compensation in favor of free credit monitoring, even if they *already* had it. In a blog post, the FTC told consumers that, because an "unexpected number" of victims filed claims, "each person who takes the money option will wind up only getting a small amount of money. Nowhere near the \$125 they could have gotten if there hadn't been such an enormous number of claims filed."

The government apparently failed to anticipate that, out of 147 million Americans victims, more than the maximum 248,000 who could have claimed their \$125 without reducing the award given to each person would have opted to do so. Even worse, it instituted a variety of new burdensome,

Case 1:19-cv-03297-TWT

bureaucratic steps required to claim the monetary award to nudge victims away from financial compensation.

Consumers should not have to jump through hoops to receive compensation for serious data privacy harms. The “unexpected” number of claimants in this case should strongly signal to policymakers that Americans care about the security of their personal data. Consumers intuitively know what EFF has said all along: the companies that store consumer’s personal information—often without their knowledge—have an obligation to protect it. If they don’t, they should pay for the harm that ensues. And financial penalties should be high enough to incentivize better data privacy practices in the future.

This settlement ensures neither. While it’s easy to be angry at the FTC, the problem really lies with the current state of privacy law. We have said it before and will say it again: without new privacy laws, or a change in how the courts view those harms, companies will not adequately invest in consumer privacy protection.

If Congress wants to protect consumer privacy, it should enact legislation with the following rules and protections.

Information fiduciary and national data breach notification rules

This one is simple: companies that collect your personal information should have a legal duty to protect it. A strong information fiduciary law would require that companies follow best practices and exercise care to protect user information as a matter of course—not as a negotiated settlement years later.

Private right of action and real damages

We need to ensure a direct, private cause of action for data breaches and other digital privacy harms to give victims a more reasonable day in court than they have now. Because data harms can be hard to quantify financially, the law should provide statutory or liquidated damages, like it does for illegal wiretapping, where Congress long ago recognized that there should be no requirement to show financial harm in order to recover.

Data broker registration

Data brokers harvest and monetize our personal information without our knowledge or consent. Worse, many data brokers fail to securely store this sensitive information, predictably leading to data breaches. One good way to facilitate better oversight comes from Vermont's new data privacy law, which requires data brokers to register annually with the government.

Non-discrimination rules

Pay-for-privacy is unfair. The law should prohibit companies from denying services, charging different prices, providing different quality levels, or otherwise discriminating against users who choose more private options.

Stronger rule-making authority for the FTC

Federal regulators must have the authority and funding to write and enforce consumer privacy rules. Congress should empower the FTC—an expert agency once tasked with data privacy regulation—to set and enforce sound security standards.

No federal pre-emption

Federal law should set a floor—not a ceiling—for privacy protection. States, as our “laboratories of democracy,” must retain their power to respond to technological changes and constituent concerns by enacting innovative data security policies.

No new criminal liability

And finally, one thing to avoid: existing computer crime laws are already extremely unfair and overbroad. That causes real harm and injustice. It also threatens the very security researchers—like the one who found an Equifax bug before the breach—who work to protect the rest of us. Any new efforts to address data breaches should focus on incentives to protect data rather than further expanding criminal liability for coders.

It has become increasingly clear that the Equifax settlement is inadequate for both compensating victims and preventing future harms. But future settlements won't be better without changes in the law or in how courts treat privacy harms. U.S. privacy law does not even give FTC the power to

require direct compensation to consumers—a powerful way to make companies pay consumers for the harm they caused. The FTC only secured it this time because individual suits were joined to its actions. Bottom line: we can't expect the current, limited-power FTC to clean up the messes created by our failure to require stronger data protections.

Our legislators have an obligation to enact the stronger data privacy protections that their constituents want and deserve.

Note: Thanks to EFF Legal Intern Victoria Noble for help with this update.

JOIN EFF LISTS

Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:



RELATED UPDATES

Federal Court Rules Suspicionless Searches of Travelers'



PRESS RELEASE | NOVEMBER 12, 2019

Phones and Laptops Unconstitutional

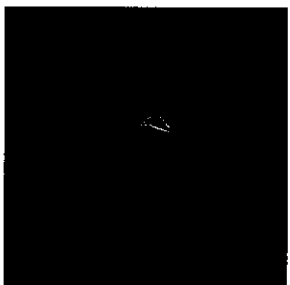
BOSTON—In a major victory for privacy rights at the border, a federal court in Boston ruled today that suspicionless searches of travelers' electronic devices by federal agents at airports and other U.S. ports of entry are unconstitutional. The ruling came in a lawsuit, *Alasaad v. McAleenan*, filed by...



PRESS RELEASE | NOVEMBER 12, 2019

EFF Sues DHS to Obtain Information About the Agency's Use of Rapid DNA Testing on Migrant Families at the Border

San Francisco—The Electronic Frontier Foundation (EFF) sued the Department of Homeland Security (DHS) today to obtain information that will shine a light on the agency's use of Rapid DNA technology on migrant families at the border to verify biological parent-child relationships. In a Freedom of Information Act (FOIA) complaint filed...



DEEPLINKS BLOG BY GENNIE GEBHART, EVA GALPERIN | NOVEMBER 6, 2019

FTC Takes Action Against Stalkerware Company Retina-X

The FTC recently took action against stalkerware developer Retina-X, the company behind apps Flexispy, PhoneSheriff, and Teenspy. The FTC settlement bars Retina-X from distributing its mobile apps until it can adequately secure user information and ensure its apps will only be used for "legitimate purposes." But here's...

Congress, Remember the 4th Amendment? It's Time to Stop the U.S.-UK Agreement.



DEEPLINKS BLOG BY JOE MULLIN | NOVEMBER 4, 2019

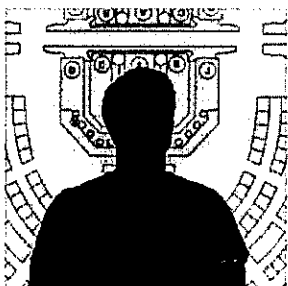
Unless Congress stops it, foreign police will soon be able to collect and search data on the servers of U.S. Internet companies. They'll be able to do it without a probable cause warrant, or any oversight from a U.S. judge. This is all happening because of a new law enforcement...



DEEPLINKS BLOG BY ADAM SCHWARTZ | OCTOBER 30, 2019

Strengthen California's Next Consumer Data Privacy Initiative

EFF and a coalition of privacy advocates recently asked the sponsor of a new California ballot initiative to strengthen its provisions on consumer data privacy. The California Consumer Privacy Act of 2018 (CCPA) created new ways for the state's residents to protect themselves from corporations that invade their...

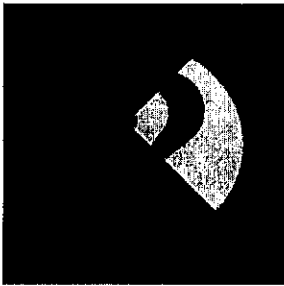


DEEPLINKS BLOG BY HAYLEY TSUKAYAMA | OCTOBER 29, 2019

Facebook Faces Another Congressional Grilling

Facebook chief executive Mark Zuckerberg was called back to Capitol Hill to speak about the company's impact on the financial and housing sectors—particularly in light of its proposal to launch a cryptocurrency wallet, Calibra, and its involvement in the creation of the Libra cryptocurrency. We've criticized Facebook on ...

Companies Can Still Do More to Protect Privacy in Brazil: Internet Lab Releases Fourth "Who Defends Your Data" Report



DEEPLINKS BLOG BY VERIDIANA ALIMONTI | OCTOBER 29, 2019
Internet Lab, the Brazilian independent research center, has published their fourth annual report of “Quem Defende Seus Dados?” (“Who defends your data?”), comparing policies of their local Internet Service Providers (ISPs) and how they treat users’ data after receiving government requests. **Vivo (Telefónica)** still takes the lead, but...



DEEPLINKS BLOG BY ERNESTO FALCON | OCTOBER 28, 2019
DNS over HTTPS Will Give You Back Privacy that Big ISPs Fought to Take Away
An absurd thing is happening in the halls of Congress. Major ISPs such as Comcast, AT&T, and Verizon are banging on the doors of legislators to stop the deployment of DNS over HTTPS (DoH), a technology that will give users one of the biggest upgrades to their Internet privacy...



PRESS RELEASE | OCTOBER 22, 2019
EFF and Partners Urge U.S. Lawmakers to Support New DoH Protocol for a More Secure Internet

San Francisco—The Electronic Frontier Foundation (EFF) today called on Congress to support implementation of an Internet protocol that encrypts web traffic, a critical tool that will lead to dramatic improvements in user privacy and help impede the ability of governments to track and censor people. EFF, joined by Consumer Reports and...

EFF Challenges Ring Spokesperson Shaq Over Privacy Concerns



**DEEPLINKS BLOG BY MATTHEW GUARIGLIA, JASON KELLEY |
OCTOBER 21, 2019**

EFF is asking Ring spokesman Shaquille O’Neal to cancel his appearance at a party hosted by the company at the upcoming International Association of Chiefs of Police conference on October 27. Instead, we’re challenging Shaq to a one-on-one: not on the basketball court, but across the table, so we can...

ELECTRONIC FRONTIER FOUNDATION
eff.org
Creative Commons Attribution License



Los Angeles Times

Log In



Case 1:19-cv-03297-TWT

ADVERTISEMENT

BUSINESS

Column: Did the FTC mislead consumers about its Equifax data breach settlement? Yes!



Equifax's reputation isn't glowing. (Justin Lane / EPA)

By MICHAEL HILTZIK
BUSINESS COLUMNIST

SEP. 10, 2019
6 AM



The Federal Trade Commission is supposed to protect consumers from being deceived by businesses. But what happens when the FTC itself is the

deceiver?

That question arises in connection with to with a new wrinkle in the settlement of up to \$700 million that the agency and other regulators reached in July with Equifax, a credit bureau that allowed the personal data of as many as 145 million consumers to be breached by hackers.

Thousands, and perhaps millions, of victims are just now discovering that they'll have to jump through an unexpected hoop if they wish to take advantage of a \$125 settlement payout that's one of the options for compensation.

It appears the agency itself may have misled the American public about the terms of the Equifax settlement and their ability to obtain the full reimbursement to which they are entitled.

SEN. ELIZABETH WARREN, D-MASS.

The discovery has come through an email sent to applicants by the settlement administrators, threatening to deny their applications for the cash payout if they don't respond with some personal information by Oct. 15. The email is sufficiently generic that it might be deleted, whether automatically or by a recipient's choice, as spam. That's what happened to two separate emails sent to my household.

ADVERTISEMENT

The FTC knows the email looks bogus. In a Q&A on its [web page detailing the settlement](#), it acknowledges that consumers might ask: "I got an email about the settlement. Is it legit?" Its answer is "Yes."

Column: Here are all the ways the Equifax data breach is worse than you can imagine

Sep. 8, 2017

This is only the latest bait-and-switch connected with the Equifax settlement, which was announced July 22 and billed as the largest such settlement ever in a data breach case. The settlement covered claims made against Equifax by the FTC, the Consumer Financial Protection Bureau and 50 states and territories. Like many such settlements, a big number ends up amounting to pennies on the dollar for individual victims.

The fine print in the Equifax case began to emerge almost immediately. It transpired that only \$31 million of the total settlement was allocated to the cash payout. As Sen. Elizabeth Warren (D-Mass.) observed in a blistering letter to the FTC, that would cover only 248,000 individuals, or less than 1% of the 145 million consumers affected by the breach.

If more than 248,000 requested the cash, the payout would be reduced on a pro-rata basis. If all 145 million victims requested cash, they'd each receive 21 cents. The rest of the settlement covered civil penalties and the cost of credit monitoring to be offered victims for free.

BUSINESS

Column: LifeLock offers to protect you from the Equifax breach — by selling you services provided by Equifax

Sep. 18, 2017

"It appears the agency itself may have misled the American public about the terms of the Equifax settlement and their ability to obtain the full

reimbursement to which they are entitled,” Warren wrote.

With that in mind, consumer advocates were forced to advise the victims that the alternative compensation — up to 10 years of “free monitoring of your credit report at the three credit bureaus (Equifax, Experian and TransUnion) and \$1,000,000 of identity theft insurance” — might be the better choice.

Among them was Rep. Alexandria Ocasio-Cortez (D-N.Y.), who initially advised constituents to opt for the cash, but then backtracked.

Okay everyone UPDATE on Equifax: for most people the better deal is 10 years of free credit monitoring.

There’s apparently a run on settlements so there’s anxiety people are going to get 16 cent checks. But if you choose 10 years of credit monitoring, Equifax **must** cover it.

— Alexandria Ocasio-Cortez (@AOC) July 27, 2019

The latest wrinkle involves the realization that the \$125 cash benefit was available only to people who already had credit monitoring in place (possible as a benefit from an earlier data breach permitted by our stunningly lackadaisical retailers, banks and data firms.

The FTC says it believes it has given consumers adequate notice of the terms of the deal. “We would dispute the assertion that we had not previously made clear that the alternative cash payment was for those affected consumers who already have credit monitoring,” FTC spokeswoman Juliana Gruenwald told me by email. She cited a [July 22 blog post](#) specifying that “affected consumers were only eligible for the alternative cash option if they already had credit monitoring.”

Gruenwald noted that the FTC, in a July 31 blog post, notified applicants to expect an email from the settlement administrator asking them to identify the credit monitoring service they already have.

Yet the agency's multiple web postings arguably have stoked consumer confusion. The deal, the FTC said in [a July statement](#), was for "up to 10 years of free credit monitoring OR \$125 if you decide **not** to enroll because you already have credit monitoring." What wasn't clear was that you couldn't seek the cash payout *unless* you didn't have credit monitoring already.

BUSINESS

Column: Insurance firms' blunders on long-term care insurance create disaster for millions

July 25, 2019

In yet another notice [posted on its website and dated this month](#), the agency says that the settlement includes free credit monitoring for up to 10 years and adds parenthetically: "(Previously, a cash payment was identified as an alternative to the free credit monitoring, but there are limited funds available.)"

The FTC seems to have decided that most consumers would have no trouble navigating through its multiple formulations of the settlement terms. Bad call, since the FTC itself seems to have been rather confused itself. For an agency with the job of ensuring that people aren't misled or cheated by the fine print in consumer contracts, its failure to make the terms crystal clear up front, and in **BOLD TYPE**, is inexcusable.

The bottom line is that countless Americans signed up for a \$125 cash

benefit plainly on the assumption that they'd get \$125, on the condition only that their data had been breached--which they could determine by plugging their name, address and a few other personal facts into a settlement website. Interestingly, the website currently requires applicants for the cash benefit to give the name of their existing credit monitoring service before proceeding. That's new. As recently as Aug. 3, according to a web archive, claimants who opted for the cash benefit were asked only if they wanted the money paid by check or pre-paid card.

That brings us to the email, which only showed up in my email account on Saturday. The email, which came from the Equifax Breach Settlement Administrator, informs applicants to "verify your claim for alternative compensation by providing "the name of your credit monitoring service that you had in place when you filed your claim."

BUSINESS

Column: If a \$5-billion fine won't shake Facebook, what can bring it to heel?

July 18, 2019

The email warns, "Please note that if you do not take action by October 15, 2019, your claim for alternative compensation will be denied." Applicants can still change their choice to free credit monitoring until the application deadline, next Jan. 22.

This is, of course, an ancient dodge well understood by insurance companies and other consumer-facing businesses: With every hoop claimants are forced to jump through, a certain percentage will give up. That's why the first, reflexive response by a health plan to a big claim is to deny it, forcing the

claimant to file an appeal. Then that's denied, requiring yet another appeal, and after a few months of this roundelay a sizable liability can be whittled away to nothing.

Should the nation's premier consumer watchdog be participating in what is, at heart, a scam? The email doesn't merely present a hoop to jump through, but requires consumers to rummage through their records to find the name of their credit monitoring service and submit proof that the service will remain in force for at least six months after the date they filed their initial claim.

This is a classic example of the proverbial "Hobson's choice" — a choice in which only one thing really is being offered. In other words, no choice at all. Free credit monitoring may be the right choice for many of Equifax's victims, or it might not. Quite a few victims might reasonably wonder at the value of a service being offered by the very firm that created their problem in the first place, through an inexcusably lax approach to the security of the personal data of half the residents of the United States.

Yes, the credit monitoring might be free, but it might be worth nothing. But forget about the \$125 alternative--it doesn't really exist in the real world.

The Equifax settlement is beginning to look not like a triumph of regulatory scrutiny, but just another ripoff--but government certified.

BUSINESS

NEWSLETTER

Get our weekly California Inc. newsletter

Please enter your email address

Subscribe

Michael Hiltzik



Twitter



Instagram



Email



Facebook

Pulitzer Prize-winning journalist Michael Hiltzik writes a daily blog appearing on latimes.com. His business column appears in print every Sunday, and occasionally on other days. As a member of the Los Angeles Times staff, he has been a financial and technology writer and a foreign correspondent. He is the author of six books, including “Dealers of Lightning: Xerox PARC and the Dawn of the Computer Age” and “The New Deal: A Modern History.” Hiltzik and colleague Chuck Philips shared the 1999 Pulitzer Prize for articles exposing corruption in the entertainment industry.

MORE FROM THE LOS ANGELES TIMES**CALIFORNIA****Sweeping bill on independent contractors passes California state Senate**

Sep. 10, 2019